AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41

I, Ronald Morin, being first duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations (HSI), and have been so employed since May 2006. I am currently assigned to the Manchester, New Hampshire field office. As part of my regular duties as an agent, I investigate criminal violations relating to a broad range of immigration and customs related statutes, including those relating to child exploitation and child pornography. I have received training in the area of child pornography and child exploitation, and as part of my duties have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in various forms of media, including digital/computer media. I have conducted investigations and executed search warrants involving child exploitation and child pornography offenses.

2. As a federal agent, I am authorized to investigate violations of the laws of the United States, and to execute warrants issued under the authority of the United States.

3. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—seven electronic devices seized from Jose Rodriguez-Garcia on June 6, 2024 —which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

4. The property to be searched are seven electronic devices seized from Jose Rodriguez-Garcia on June 6, 2024:

a. Two Samsung cellular smartphones, one black in color and one silver in color;

b. Three SIM Cards, consisting of one V8.5R SIM and two Lucky Mobile SIM; and

c. Two thumb drives, consisting of one silver 16GB USB thumb drive, and one blue Samsung 64 USB 3.1 thumb drive.

The above seven items are collectively referred to as the "Subject Devices." All of the Subject Devices are currently in the custody of HSI at 275 Chestnut Street, Suite 307, Manchester, NH 03101. The applied-for warrant would authorize the forensic examination of the Subject Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

STATUTORY AUTHORITY

5. Title 18, United States Code, Section 2252(a)(1) and (b)(1) prohibit any person from knowingly transporting any visual depiction in interstate or foreign commerce by any means if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

6. Title 18, United States Code, Section 2252(a)(4)(B) and (b)(2) prohibit any person from knowingly possessing or accessing with the intent to view, or attempting or conspiring to possess or access with the intent to view, 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or

has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

7. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

8. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

PROBABLE CAUSE

9. On June 6, 2024, at approximately 5:45 AM Unites States Border Patrol agents received a call from an off-duty Border Patrol Agent stating that he saw two individuals on bicycles, carrying backpacks, traveling south on Hall Stream Road in Beecher Falls, VT. Agents located the two individuals—two men on bicycles—at approximately 6:00 AM, just west of the

town of Beecher Falls, VT. Both men had wet shoes at the time, indicating that they had possibly crossed from Canada into the United States by traversing Hall Stream.

10. When agents asked as to their citizenship both men stated that they were citizens of Mexico. They also freely admitted that they had just crossed illegally from Canada into the United States by crossing the water. The man ultimately identified as Jose Rodriguez-Garcia had one of the two Samsung phones identified above displaying GPS on his bicycle which an agent observed had markers from Montreal, Canada to Montpelier, VT. Notably there was a marked point on Hall Stream in Pittsburg, NH, where the men appeared to have crossed the border from Canada into New Hampshire. The subjects were detained, taken into custody and transported to Beecher Falls Border Patrol Station, Vermont, for processing on suspected violations of 8 U.S.C. § 1325, regarding improper entry.

11. During processing at the station, the men identified themselves as Rodriguez-Garcia and his brother. These identifications were consistent with Mexico voter-identification cards in their possession.

12. A search of Rodriguez-Garcia's belongings was conducted for prohibited items and to dispose of any wet articles and clothing. Rodriguez-Garcia was in possession of the two Samsung phones identified above. When arrested, Rodriguez-Garcia was wearing a black fanny pack, which was wet. Inside the fanny pack, agents found a small red container, inside of which were the two thumb drives and three SIM cards. Agents attempted to do a border search review of the media, starting with one of the two thumb drives. On the silver 16 GB thumb drive, the reviewing agent encountered travel documents relating to Mexico and Canada containing Rodriguez-Garcia's name. The agent additionally discovered video files of what appears to be nude pre-pubescent girls engaged in sex acts with what appears to be an adult male. Upon these

discoveries, the reviewing agent stopped the search of the thumb drive.

13. The videos that were discovered were additionally reviewed by my colleagues Brian Wilda and Jamie West of HSI, who described them as follows:

a. File Name: VID-20230403-WA0097. This video is approximately 59 seconds in length. There is a female laying on a blue bed sheet wearing only a purple shirt. Her face is visible. She appears to be under the age of 12. She is naked from the waist down and her legs are spread open revealing her vagina. There is no visible pubic hair. There is an adult male who is rubbing his erect penis on the female vagina and masturbating. At one point, the male uses his fingers to further expose the female's vagina.

b. VID-20230405-WA0048. This video that is approximately 31 seconds in length. There is a nude adult male and a nude female in the video. The female appears to be approximately 12 years old. Her face is visible. She has no visible pubic hair and no visible breast development. She is laying on her back on what appears to be a bed. The entire video shows the adult male having vaginal intercourse with the female.

14. Therefore, the two observed videos appeared to meet the statutory definitions of child pornography and sexually explicit conduct identified above.

15. Rodriguez-Garcia was provided *Miranda* warnings in Spanish language using a telephonic interpreter and stated that he understood his rights and waived them through the interpreter. In post *Miranda* waiver questioning, Rodriguez-Garcia described and showed agents where he entered into the United States on an online map, specifically pointing out his crossing location in Pittsburg, New Hampshire.

16. Agents Wilda and West conducted an additional interview later on June 6, 2024, again utilizing a Spanish language telephonic interpreter, and Rodriguez-Garcia acknowledged that the black fanny pack and its contents belonged to him.

17. Rodriguez-Garcia was subsequently charged by complaint with violating 18 U.S.C. § 2252(a)(1) regarding the transportation of child pornography and 18 U.S.C. § 2252(a)(4)(B) regarding the possession of child pornography.

18. The Subject Devices are currently in the lawful possession of the HSI. While HSI may already have all necessary authority to examine the Subject Devices, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Subject Devices will comply with the Fourth Amendment and other applicable laws.

19. The Subject Devices are currently in storage at HSI in Manchester, NH. In my training and experience, I know that the Subject Devices have been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when they first came into the possession of Border Patrol and HSI.

TECHNICAL TERMS

20. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually

contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store

other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless

communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and

international borders, even when the devices communicating with each other are in the same state.

h. A "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, "thumb," "jump," or "flash" drives, CD-ROMs, and other magnetic or optical media.

i. A SIM ("Subscriber Identity Module") card is an integrated circuit intended to securely store an international mobile subscriber identity (IMSI) number and its related key, which are used to identify and authenticate subscribers on mobile telephone devices (such as mobile phones and laptops). The SIM also stores phone directories, messages, information on roaming across different networks, and many other value-added voice and data services. This information is important in establishing users who may have shared files and network information that may establish location/travel information.

21. Based on my training, experience, and research, I know that the seized Samsung phones have the capabilities to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, Internet access device and PDA. The two thumb drives can maintain digital files placed there by the user, and the SIM cards have the capabilities identified above. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the devices.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

22. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. With regard to the two Samsung phones, similarly, things that have been viewed via the Internet are typically stored for some period of time on each device. This information can sometimes be recovered with forensics tools.

23. With regard to the SIM cards and thumb drives, there is probable cause to believe that things that were once stored on those devices may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

24. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

25. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but

not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

26. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

27. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

/s/ Ronald Morin
Ronald Morin
Special Agent
Homeland Security Investigations

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. Crim. P. 4.1 and affirmed under oath the content of this affidavit and application.

Date: **Jun 14, 2024**
Time: **12:15 PM, Jun 14, 2024**

HONORABLE ANDREA K. JOHNSTONE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

28. The property to be searched are seven electronic devices (the "Subject Devices") seized from Jose Rodriguez-Garcia on June 6, 2024, and in the custody of HSI at 275 Chestnut Street, Suite 307, Manchester, NH 03101:

a. Two Samsung cellular smartphones, one black in color and one silver in color;

b. Three SIM Cards, consisting of one V8.5R SIM and two Lucky Mobile SIM; and

c. Two thumb drives, consisting of one silver 16GB USB thumb drive, and one blue Samsung 64 USB 3.1 thumb drive.

This warrant authorizes the forensic examination of the Subject Devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

All records on the Subject Devices described in Attachment A which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2252(a)(1) and (a)(4)(B), including:

a. records and visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256;

b. records or information pertaining to an interest in child pornography;

c. records or information pertaining to the possession, receipt, transportation, or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

d. records or information of and relating to visual depictions that have been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct as defined in 18 U.S.C. § 2256, including the record or information used to create the visual depiction;

e. photo-editing software and records or information relating to photo-editing software;

f. records or information relating to the ownership, possession, or use of the Subject Devices.

2. For any computer, computer hard drive, or other physical object upon which electronic data can be recorded (hereinafter, "COMPUTER") that is called for by this warrant, or that might contain things otherwise called for by this warrant:

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

f. evidence of the times the COMPUTER was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

i. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

As used above, the term "COMPUTER" includes but is not limited to any and all computer equipment, including any electronic devices that are capable of collecting, analyzing, creating, displaying, converting, storing, concealing, or transmitting electronic, magnetic, optical, or similar computer impulses or data. These devices include but are not limited to any data-processing hardware (such as central processing units, memory typewriters, mobile "smart"

telephones, tablets, and self-contained "laptop" or "notebook" computers); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives and diskettes, thumb drives, flash drives, Micro SD cards, SD cards, CDs, DVDs, tape drives and tapes, optical storage devices, zip drives and zip disk media, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, fax machines, digital cameras, scanners, plotters, video display monitors, and optical readers); and related communications devices (such as modems, routers, cables and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone-generating devices); as well as any devices, mechanisms, or parts that can be used to restrict access to such hardware (such as physical keys and locks).